REMARKS

Favorable reconsideration of this application, in light of the preceding amendments and following remarks, is respectfully requested.

Claims 21-40 are pending in this application. By this amendment, claims 21-40 are amended. No new matter is added. Claims 21 and 39 are the independent claims.

Applicants note with appreciation the Examiner's acknowledgement that certified copies of all priority documents have been received by the U.S.P.T.O.

Applicants also appreciate the Examiner's indication that the Information Disclosure Statement (IDS) filed on April 26, 2006, has been considered.

Applicants also respectfully note the present action indicates that the drawings have been accepted by the Examiner.

Objection to the Specification

The specification is objected to because the abstract consists of more than 150 words. Applicants hereby submit a new abstract consisting of less than 150 words, and respectfully request that the objection to the specification be withdrawn.

Objection to the Drawings

The drawings are objected to under 37 C.F.R. § 1.83(a) for not showing every feature of the invention specified in the claims, with respect to the cryptogram.

Applicants submit that the cryptogram is clearly shown in FIG. 1 as a small circle labeled "J" travelling from the control server (CSE) to the net (NET), and is also shown as a small circle labeled "J" travelling from the mobile equipment (CB) to the

Subscriber Identity Module (SIM). Thus, Applicants respectfully request that the objection to the drawings be withdrawn.

Objection to the Claims

Claims 21 and 26 are objected to regarding informalities with respect to clarity and antecedent basis. By the instant amendment, claims 21 and 26 have been amended, taking into account the Examiner's suggestions, to remedy the objections. Withdrawal of the objections is respectfully requested.

Rejections under 35 U.S.C. § 112

Claims 25 and 34 are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite with respect to antecedent basis. Applicants submit that this rejection has been overcome by the foregoing amendments. Thus, Applicants respectfully request that this rejection of the claims be withdrawn.

Rejections under 35 U.S.C. § 102

Claims 21-36 and 38-40 are rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent 5,864,757 ("Parker"). Applicants respectfully traverse this rejection for the reasons detailed below.

In order to establish anticipation under 35 U.S.C. § 102, each and every element as set forth in the rejected claim must be found, either expressly or inherently described, in a single prior art reference.[1] Applicants respectfully submit that the cited art does not meet these criteria, because Parker does not describe all of the elements of rejected claims 21-36 and 38-40, and therefore these claims are not anticipated.

For example, independent claim 21, as amended, recites, "**selectively activating or selectively deactivating by the security module at least one resource** as data or functions of said security module by executing instructions included in the cryptogram and conditioning the functioning of an application according to criteria established by at least one of a supplier of said application, the operator and a user of the equipment."

Claim 21 has been amended to clarify the scope to **selective activation or selective deactivation** of resources in the security module, for example by taking account of functionalities of a particular application without blocking the possibility of connecting the equipment to the network. For support, see, e.g., paragraph [0015] of the Substitute Specification of the present application filed on April 26, 2006, which states: "*The resources of the subscriber module are blocked in a targeted way, in order to block or reduce the function of certain applications. The applications of the equipment are not directly blocked: one act indirectly on the applications, that is to say that the blocking effect will be noticed only when the equipment attempts to carry out these applications*"

In contrast, Parker merely describes a method for activating a mobile handset including a subscriber or security module as a SIM card. The method of Parker is based on using a unique inviolable key specific to the handset, whereby the key provides a code corresponding to an identifier of the subscriber module. During activation of the handset, the managing center of the operator sends a message to the handset allowing calculating a key specific to the operator by using the unique key of the handset. This new key is combined with a network identifier or with the subscriber module identifier for generating a control word which is confronted to a code stored in

[1] See *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d

the subscriber module. If the control word matches with the code of the subscriber module, the handset is activated.

Therefore, the aim of this method of Parker is to lock or unlock a mobile equipment (or rather the security module of the mobile equipment) to all services provided by a predetermined operator. In this case, the security module is also activated or deactivated in its entirety in order to be compatible with the characteristics of the services of a given provider.

To summarize, **Parker requires that the message** sent to the security module via the handset **deactivates or activates the entire security module**.

In contrast to Parker, **claim 21 requires** that the cryptogram **selectively** activates or **selectively** deactivates at least one resource. In fact, Parker does not mention any selective or targeted effect of the message on specific functionalities or resources of the security module used by applications. The method of Parker is focused on the switching on or off the security module as a function of the presence or the absence of the subscriber module identifier or corresponding code in a database.

In addition, the method of claim 21 does **not** lock the security module, i.e. the mobile equipment remains able to connect to the network and to communicate in a standard manner. According to the method of claim 21, for example, only one or several applications work in a reduced way in the absence of sufficient resources in the security module, these resources having been deactivated by the message. An application may correspond to an additional value added service such as: the consultation of various information, remote banking operations, the electronic commerce, access to multimedia content, etc. The functions of the resources attached to these applications may comprise: cryptographic algorithms, digital signatures

---

1051, 1053 (Fed Cir. 1987).

generating processes, access control processes, payment processes etc. The message sent by the managing center according to claim 21 may deactivate, for example, an algorithm or a cryptographic key stored in the security module in order to disable a remote payment application. The other applications, for example the consulting of stock exchange information, which do not require the key or algorithm in question, will still work normally because they have sufficient active resources in the security module.

In other words, the method of Parker merely acts as an on/off mode, wherein the security module is either entirely locked or entirely unlocked. In contrast to Parker, the method of **claim 21 selectively** activates or **selectively** deactivvates the resources of predetermined applications.

Therefore, Applicants respectfully submit that the teaching of Parker are insufficient for disclosing a method for selective managing of the security of applications in a mobile equipment. Parker does not disclose applications installed in the mobile equipment using resources of the security module. Parker merely discloses that the activating operation (when the control word matches with the code of the subscriber module) acts as a starting switch for the mobile equipment which can connect to the network.

According to claim 21, the message (cryptogram) may include instructions providing results conditioning the functioning of applications by limiting or by extending their functionalities according to criteria predetermined by the provider of said application or the operator or the user of the mobile equipment.

Since the rejection fails to set forth every element of claim 21, Applicants submit that claim 21 is not anticipated by Parker.

Further, independent claim 39, as amended, recites, *inter alia*:

> the security module further comprises means for receiving and analyzing a cryptogram and **means for selectively activating or selectively deactivating at least one resource** as data or functions of the security module by executing instructions included in the cryptogram and conditioning the functioning of an application according to criteria predetermined by at least one of the supplier of said application, the operator and a user of the equipment.

Thus, Applicants submit that independent claim 39 is not anticipated by Parker for at least similar reasons as independent claim 21.

Claims 22-38 and 40, dependent on independent claims 1 and 39, are patentable for the reasons stated above with respect to claims 21 and 39, as well as for their own merits.

Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection to independent claim 1 and 39, and all claims dependent thereon.

Rejections under 35 U.S.C. § 103

Claim 37 is rejected under 35 U.S.C. § 103 as being obvious over U.S. Patent 5,864,757 ("Parker") in view of U.S. Patent Application Publication 2003/0041125 ("Salomon"). Applicants respectfully traverse this rejection for the reasons detailed below.

In order to establish *prima facie* obviousness under 35 U.S.C. § 103(a), all the claim limitations must be taught or suggested by the prior art. As discussed above, Parker does not disclose all of the elements of independent claim 21. Further, Applicants submit that Salomon does not remedy the deficiencies of Parker. Specifically, Salomon merely discloses a receipt of files message, and does not teach or suggest "**selectively activating or selectively deactivating by the security module at least one resource,**" as required by independent claim 21.

Thus, Applicants submit that independent claim 21 is non-obvious over the combination of Parker and Salomon. If an independent claim is non-obvious, then any claim depending therefrom is non-obvious.[2]

Therefore, Applicants submit that dependent claim 37 is non-obvious for at least similar reasons as independent claim 21, and respectfully request that the rejection to claim 21 under 35 U.S.C. § 103 be withdrawn.

CONCLUSION

Accordingly, in view of the above amendments and remarks, reconsideration of the objections and rejections and allowance all pending claims in connection with the present application is earnestly solicited.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact the undersigned, at the telephone number below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. §1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By _____

John A. Castellano, Reg. No. 35,094

P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

JAC/EGO/DJC/dmc

[2] See *In re Fine*, 837 F. 2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).